AMENDMENTS TO THE CLAIMS

The following is a complete, marked-up listing of revised claims with a status identifier in parenthesis, underlined text indicating insertions, and strike through and/or double-bracketed text indicating deletions.

LISTING OF CLAIMS

1.-16. (CANCELLED)

17. (Currently Amended) ~~Validity verification method for~~ A method for verifying validity of a network key in a digital domestic network comprising at least a broadcasting device and ~~a~~ at least one processing device, the broadcasting device ~~having encrypted data to broadcast to the processing device, these data being accessible by the processing device thanks~~ transmits to the processing device encrypted data, the data being accessible by the processing device due to a network key unknown by the broadcasting device, ~~this method comprising following steps:~~ the method comprising:

transmitting by the broadcasting device a test key to the processing device,

receiving from the processing device a cryptogram made up of the test key encrypted by the network key, and

determining the validity of the network key by comparing the received cryptogram with at least one of a plurality of control cryptograms taken from a list of control data generated by a verification center for the test key.

~~transmission of a test key by the broadcasting device to the processing device,~~

~~calculation of a cryptogram in the processing device resulting from the test key encryption by the network key,~~

~~sending of the cryptogram to the broadcasting device,~~

~~determination of the network key validity by the broadcasting device by comparing the cryptogram with a list of control cryptograms.~~

18. (Currently Amended) ~~Verification~~ The method according to claim 17, wherein the test key and the ~~list of~~ control cryptograms ~~constitute control data and~~ are generated ~~in a~~ by the verification center and transferred ~~in~~ to the broadcasting device.

19. (Cancelled)

20. (Currently Amended) ~~Verification~~ The method according to claim ~~19~~ 17, wherein the test key is randomly generated by the broadcasting device and used ~~and serves also~~ as session key for the encryption of the encrypted data.

21. (Currently Amended) ~~Verification~~ The method according to claim ~~19~~ 20, wherein the broadcasting device generates at least two test keys and ~~transmit them~~transmits the at least two test keys to the processing device, ~~which sends back to it~~ received from the processing device the corresponding cryptograms, selects one control cryptogram from the list of control data and the ~~and it's~~ associated test key for the verification operations and ~~an other~~ another control cryptogram and ~~its~~ the associated test key as session key for the encryption of the data encryption.

22. (Currently Amended) ~~Verification~~ The method according to claim 18, wherein the ~~list of~~ control cryptograms ~~consists of a~~ are in a black list containing ~~the~~ cryptograms obtained by the ~~encryption of~~ encrypting the test key with invalid network keys.

23. (Currently Amended) ~~Verification verification~~ The method according to claim 18, wherein the ~~list of~~ control cryptograms ~~consists of a white list~~ are in a white list containing the cryptograms obtained by the ~~encryption of~~ encrypting the test key with valid network keys.

24. (Currently Amended) ~~Verification verification~~ The method according to claim 22, wherein ~~a cryptogram present in the black list or absent from the white list is refused during the comparison,~~ an error signalization inviting the user to change the terminal module is ~~then generated~~ generated when a received cryptogram is present in the black list and refused during the comparison.

25. (Currently Amended) ~~Verification~~ The method according to claim 17, wherein the broadcasting device comprises a converter module in charge of the verification operations.

26. (Currently Amended) ~~Verification~~ The method according to claim 17, wherein the processing device comprises a terminal module storing the network key.

27. (Currently Amended) ~~Verification~~ The method according to claim ~~25,~~ 28, wherein the control ~~list is~~ cryptograms are stored in a memory of the broadcasting device, and the comparison with the received cryptogram is carried out by ~~this~~ the broadcasting device.

28. (Currently Amended) ~~Verification~~ The method according to claim ~~19,~~ 17, wherein the control data ~~consist of~~ includes an address indicating where the control ~~list~~ cryptograms can be downloaded via Internet by ~~means of~~ the broadcasting device, ~~said list is then~~ the control cryptograms being stored in the memory of the broadcasting device.

29. (Currently Amended) ~~Verification~~ The method according to claim ~~25,~~ 28 wherein the converter module verifies the authenticity of the ~~control~~ list of control data ~~by means of~~ via a signature on ~~said~~ the data.

30. (Currently Amended) ~~Verification~~ The method according to claim 17, wherein the control ~~list is stored by a~~ data is generated in the verification center, the broadcasting device transmits the received control cryptogram ~~to said center~~ and the locally generated test key to the verification center for carrying out the verification.

31. (Currently Amended) ~~Verification~~ The method according to claim ~~19,~~ 17, wherein the broadcasting device is a DVD disc ~~reader,~~ reader for reading a disk, ~~this~~ the disc ~~comprising on one hand the~~ includes at least one of the encrypted data and ~~on the other hand the~~ the list of control data.

32. (Currently Amended) ~~Verification~~ The method according to claim ~~19,~~ 17, wherein the broadcasting device is a pay television decoder receiving the encrypted data and the list of control data from a managing center.

33. (Currently Amended) ~~Verification~~ The method according to claim 23, wherein ~~a cryptogram present in the black list or absent from the white list is refused during the comparison,~~ an error signalization inviting the user to change the terminal

module is ~~then~~ generated when a received cryptogram is absent of the white list and refused during the comparison.

34. (New) The method according to claim 18, wherein the control cryptograms are in a black list containing cryptograms obtained by encrypting the test key with invalid network keys and in a white list containing the cryptograms obtained by encrypting the test key with valid network keys.

35. (New) The method according to claim 26, wherein an error signalization inviting the user to change the terminal module is generated when a received cryptogram is present in the black list or absent of the white list, the received cryptogram being refused during the comparison.

36. (New) The method according to claim 17 wherein the list of control data is generated in the verification center, the broadcasting device transmits the received control cryptogram generated by the processing device based on the test key received by the broadcasting device from the verification center, the verification center carrying out the verification.